Automatica 49 (2013) 2373–2383

Contents lists available at SciVerse ScienceDirect

Automatica

journal homepage: www.elsevier.com/locate/automatica

Optimal sensor selection for ensuring diagnosability in labeled Petri nets☆

Maria Paola Cabasino [a,1], Stéphane Lafortune [b], Carla Seatzu [a]

[a] Department of Electrical and Electronic Engineering, University of Cagliari, Italy

[b] Department of Electrical Engineering and Computer Science, University of Michigan, MI, USA

ARTICLE INFO

Article history:
Received 26 July 2012
Received in revised form
21 January 2013
Accepted 23 April 2013
Available online 29 May 2013

Keywords:
Petri nets
Place/transition nets
Discrete event systems
Fault diagnosis

ABSTRACT

This paper studies the problem of optimal static sensor selection for ensuring diagnosability in labeled bounded and unbounded Petri nets. Starting from a non-diagnosable labeled Petri net system, we present a systematic procedure to design a new labeling function that makes the system diagnosable and optimizes a given objective function. This procedure employs a particular net, called Verifier Net, that is built from the original Petri net and provides necessary and sufficient conditions for diagnosability. We exploit the system structure captured in the verifier net to guide the search for the desired new labeling function. The search is performed over an unfolding of the reachability/coverability tree of the verifier net and follows a set of rules that capture the relabeling strategy. We allow for unobservable transitions that cannot be labeled as well as for multiple fault classes. We formulate an integer linear programming problem that finds an optimal labeling function when numerical costs are associated with transition relabeling.

1. Introduction

We study the problem of optimal static sensor selection for ensuring diagnosability of a labeled Petri net system. The analysis of the diagnosability properties of Petri net systems has been addressed in several works, including (Cabasino, Giua, Lafortune, & Seatzu, 2012; Chung, 2005; Haar, 2009; Jiroveanu & Boel, 2010; Madalinski, Nouioua, & Dague, 2010; Ushio, Onishi, & Okuda, 1998). On the other hand, very few results are available regarding the sensor selection problem for ensuring diagnosability in the context of Petri net systems. A labeled Petri net dynamic system is diagnosable if every occurrence of an unobservable fault transition can be detected within a finite number of transition firings, based on observed transition labels. We start from a Petri net whose set of transitions is divided into observable and unobservable transitions and whose observable transitions may share the same label. Each transition represents a physical event in the system to which a sensor could potentially be attached. We assume that a subset of the unobservable transitions may not be labeled, i.e., they cannot be made observable. We assume that the given Petri net system is not diagnosable under a given initial transition labeling function. Our goal is to design a new labeling function that makes this system diagnosable. We start from the reachability or coverability graph (RG/CG) of a particular Petri net called Verifier Net (VN); RG is used in the bounded case and CG is used in the unbounded case. The RG/CG of the VN gives necessary and sufficient conditions for diagnosability, as studied in Cabasino, Giua et al. (2012). After we unfold the RG/CG of the VN, we select all elementary paths, called elementary bad paths, that lead to a violation of diagnosability. We use the results in Cabasino, Giua et al. (2012) to identify such paths. We prove that if we relabel at least one transition (unobservable that can be labeled or observable and indistinguishable) in each elementary bad path following some relabeling rules, then we obtain a Petri net that is diagnosable under the new labeling function. This approach does not require iterations to identify a set of sensors that render the system diagnosable. Moreover, it leads directly to the formulation of an optimization problem for finding an optimal relabeling, given the individual relabeling costs of transitions.

Related problems on optimal static sensor selection have been addressed in Aguirre-Salas (2003), Bavishi and Chong (1994), Debouk, Lafortune, and Teneketzis (2002), Haji-Valizadeh and Loparo (1996), Jiang, Kumar, and Garcia (2003) and Ru and Hadjicostis

☆ This work was partially supported by the Research Project supported by Region Sardinia, L.R. 7/2007, Basis Research - Call 2008 and by the US National Science Foundation (Grant CNS-0930081). The material in this paper was presented at the 11th IFAC International Workshop on Discrete Event Systems (WODES 2012), October 3–5, 2012, Guadalajara, Mexico. This paper was recommended for publication in revised form by Associate Editor Jan Komenda under the direction of Editor Ian R. Petersen.

E-mail addresses: cabasino@diee.unica.it (M.P. Cabasino), stephane@eecs.umich.edu (S. Lafortune), seatzu@diee.unica.it (C. Seatzu).

[1] Tel.: +39 0706755773; fax: +39 0706755782.

0005-1098/$ – see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.automatica.2013.04.041

(2010). The main goal in Bavishi and Chong (1994), Debouk et al. (2002), Haji-Valizadeh and Loparo (1996), and Jiang et al. (2003) is similar to the one considered in this paper; however these works consider a finite state automaton model of the system. The use of labeled Petri nets allows for general relabeling when solving the sensor selection problem. For instance, if two or more observable transitions share the same label and we wish to relabel one or more of them, several options are available. When solving sensor selection problems with automata models, the choice is typically to make an unobservable event observable, since labels are associated with events, not transitions. Therefore, an approach that works directly with the labeling of the Petri net transitions will lead to different solutions as compared with an approach that would build the reachability graph of the (bounded) net and then employ one of the above automata-based techniques.

In the framework of Petri nets, some results have been presented for the optimal sensor selection problem, but the goal was to achieve structural observability, not diagnosability. In Ru and Hadjicostis (2010), the authors want to find a place sensor configuration and a labeling function such that a partially observed Petri net is structurally observable, namely, given an arbitrary but known initial state M_0 and any firing sequence from M_0, the system state at any given time step can be determined uniquely based on observations from place sensors and transition sensors up to that time step. The authors consider the two subproblems (optimal place sensor selection and optimal transition sensor selection) separately. In Aguirre-Salas (2003), the authors study an optimal sensor selection problem for observability in Interpreted Petri nets (IPNs) using a genetic approach. This approach takes advantage of the characterization of event-detectability and marking-detectability for live, conservative and cyclic IPNs. The problem statement in our case differs from the ones of Aguirre-Salas (2003) and Ru and Hadjicostis (2010): they deal with (structural) observability while we deal with diagnosability.

The main contributions of this paper are characterized as follows. First, we use the fact that the VN provides necessary and sufficient conditions for diagnosability for both bounded and unbounded Petri nets. Then, we exploit the system structure captured in the VN to guide the search for the desired new labeling function. In other words, as will become clear later, the *violations* of diagnosability, as captured in the VN, guide the selection of the transitions to be relabeled, i.e., that acquire their own sensor. For this purpose, we present a set of *labeling rules* that should be followed. Given these rules, we show that the labeling function selection problem has a natural formulation as an optimization problem, given the costs of attaching sensors to transitions. In this regard, we formulate an integer linear programming problem (ILPP).

A preliminary and partial version of this paper was presented in Cabasino, Lafortune, and Seatzu (2012). Specifically, in Cabasino, Lafortune et al. (2012), we consider the same problem statement, but restrict attention to bounded nets and single fault classes and assume that all unobservable transitions can be relabeled. Here, these assumptions are relaxed. Moreover, we present all proofs, the complete ILPP formulation and solution of the transition labeling optimization problem (Section 5), and the analysis of the computational complexity of the procedure (Section 6); these are not available in Cabasino, Lafortune et al. (2012). Finally, all examples and Section 3.3 are also new.

The presentation is organized as follows. In Section 2, we present necessary background on labeled Petri nets. In Section 3, we first introduce the notion of diagnosability; then we present the problem statement, the assumptions on which our approach is based, and some motivational examples. For simplicity, we consider bounded Petri nets first. We also prove the monotonicity property of relabeling in that section. In Section 4, we prove the correctness of the proposed procedure. In Section 5, we show how to implement our approach by solving an integer linear programming problem. In Section 6, we discuss the computational complexity of the proposed procedure. In Section 7, we consider the case of multiple fault classes and the case of unbounded nets. Section 8 concludes the paper.

2. Background on labeled Petri nets

In this section we recall notation and basic concepts about Petri nets. For more details, refer to Cassandras and Lafortune (2007), Hrúz and Zhou (2007) and Murata (1989).

A *Place/Transition net* (P/T net) is a structure $N = (P, T, Pre, Post)$, where P is the set of m places, T is the set of n transitions, $Pre : P \times T \to \mathbb{N}$ and $Post : P \times T \to \mathbb{N}$ are the pre and post incidence functions that specify the arcs. The function $C = Post - Pre$ is called the incidence matrix. A *marking* is a vector $M : P \to \mathbb{N}$ that assigns to each place a nonnegative integer number of tokens; the marking of a place p is denoted by $M(p)$. A *net system* $\langle N, M_0 \rangle$ is a net N with an initial marking M_0.

A transition t is enabled at M iff $M \geq Pre(\cdot, t)$ and may fire yielding the marking $M' = M + C(\cdot, t)$. The notation $M[\sigma\rangle$ is used to denote that the sequence of transitions $\sigma = t_1 \ldots t_k$ is enabled at M; moreover we write $M[\sigma\rangle M'$ to denote the fact that the firing of σ from M yields to M'. Given a sequence $\sigma \in T^*$ we write $t \in \sigma$ to denote that a transition t is contained in σ. We denote by $|\sigma|$ the length of the sequence σ. The set of all sequences that are enabled at the initial marking M_0 is denoted by $L(N, M_0)$.

A marking M is said to be *reachable* in $\langle N, M_0 \rangle$ if there exists a firing sequence σ such that $M_0[\sigma\rangle M$. The set of all markings reachable from M_0 defines the *reachability set* of $\langle N, M_0 \rangle$ and is denoted by $R(N, M_0)$. $\langle N, M_0 \rangle$ is said to be bounded if there exists a positive constant k such that for all $M \in R(N, M_0)$, $M(p) \leq k$.

A *labeling function* $\mathcal{L} : T \to L \cup \{\varepsilon\}$ assigns to each transition a symbol from a given alphabet L or the empty string symbol ε. We call *labeled Petri net system* the triple $\langle N, M_0, \mathcal{L} \rangle$. We denote as $\mathcal{L}^{-1}$ the inverse operator of $\mathcal{L}$. The set of transitions sharing the same label l is denoted by T_l. Given a language $L(N, M_0) \in T^*$, we denote by $L(N, M_0)/\sigma$ the post-language of $L(N, M_0)$ after σ, i.e., $L(N, M_0)/\sigma = \{\sigma' \in T^* \mid \sigma\sigma' \in L(N, M_0)\}$.

Finally, given a net $N = (P, T, Pre, Post)$ and a subset $T' \subseteq T$ of its transitions, we define the T'-induced subnet of N as the new net $N' = (P, T', Pre', Post')$, where Pre' and $Post'$ are the restrictions of Pre and $Post$ to $P \times T'$, i.e., N' is the net obtained from N removing all transitions in $T \setminus T'$. We write that $N' \prec_{T'} N$.

3. Problem formulation

Let us consider a labeled Petri net system $\langle N, M_0, \mathcal{L}_{init} \rangle$ with an "initial" transition labeling function $\mathcal{L}_{init} : T \to L_{\text{init}} \cup \{\varepsilon\}$ that assigns to each transition a symbol from a given alphabet L_{init} or the empty string ε. Assume T is divided into two disjoint subsets: T_o, the set of observable transitions whose labels are from the set L_{init}; and T_u, the set of unobservable transitions whose labels are all equal to ε. T_u is further partitioned into two disjoint subsets: T_f, the set of *fault* transitions, and T_{reg}, the set of unobservable but regular (i.e., not faulty) transitions. The set of regular transitions is divided into two disjoint subsets: $T_{r,o}$ the set of regular transitions to which is possible to associate a sensor and $T_{r,uo}$, the set of regular transitions that cannot be labeled. We use the symbol t_f to denote a generic element of T_f. If desired, T_f can be partitioned into subsets corresponding to different fault classes, each denoted by T_f^i. We also assume that $L_{init} \cap T = \emptyset$, i.e., none of the original labels can be the name of a transition.

3.1. Notion of diagnosability

The following definition of diagnosability of Petri nets is inspired by the definition of diagnosability for (regular) languages